Balancing Your Internet Cyber-Life with Privacy and Security

Joseph Guarino
Owner/Sr. Consultant Evolutionary IT
CISSP, LPIC, MCSE 2000, MCSE 2003, PMP
www.evolutionaryit.com
in association with GBC/ACM

Often...

When I speak about security/privacy threats to non-technical customers, friends and family are incredulous.

It's almost as if I am speaking about science fiction.

Security is a real concern

unlike Bigfoot.

Frame from Patterson-Gimlin film taken on October 21st, 1967

Objectives

- Elucidate and demystify the subjects of cyber security and privacy in plain English.
- Explain why your privacy/security is important and how to protect it.
- Impart understanding of the privacy/security risks, impacts, ramifications.
- Give you practical knowledge to protect yourself, family and community.

Who am I?

- Joseph Guarino
- Working in IT for last 15 years: Systems, Network, Security Admin, Technical Marketing, Project Management, IT Management
- CEO/Sr. IT consultant with my own firm Evolutionary IT
- CISSP, LPIC, MCSE, PMP
- www.evolutionaryit.com

Computer Security

The fundamentals for the everyday users.

Common Misperceptions

- *“I have anti-virus software...”*
- *“I don't personally have anything of value on my computer...”*
- *“I have a firewall...”*
- *“There are no major financial risks...”*

Key terms/concepts

Define some key terms...

General Terms

- **Software Bug** – an error, flaw or mistake in a computer program.
- **Vulnerability** – is a weakness in a system that allows an attacker to exploit or otherwise violate the integrity of your system.
- **Patch** – a fix for a software bug or security vulnerability.

Malware Terms

- **Malware** – software designed to infect and damage a user's computer system without the owner's consent. This is the general all encompassing term.
- **Virus** – computer program that infects or copies itself onto a user's computer system without user's permission/consent. Most often a virus delivers a dangerous payload or action.

Malware Terms

- **Spyware** – software installed surreptitiously on a users computer system to intercept, monitor, market.
- **Adware** – software installed surreptitiously which is designed to deliver ads.
- **Badware** – alternative term used to describe spyware, malware and deceptive adware.
- **Grayware** – term used to describe spyware, adware, dialers, remote access kits that harm systems performance.

Malware Terms

- **Bot** – machines infected with worms, trojans or other malware under a centralized control structure.
- **Worms** – network enabled or aware viruses.
- **Rats** – remote access toolkits which allow remote access to a users machine.

Malware Terms

- **Dialer** – an unwanted dial application which connects to pay-rate phone numbers.
- **Rootkits** - program that takes fundamental control of your system without your consent.
- **Key Loggers** – hardware or software means of capturing users keystrokes.
- **Phishing** – attempt via email, IM or other malware to redirect user to fraudulent websites.

Evolution of Malware

- Malware today has evolved beyond the simple virus.
- Malware's evolution will NOT stop and it will be a constant battle to defend against an ever changing threat.
- Profit motive of cyber criminals will always bring new threats.
- Consider that the threats will expand to new technologies.

Software Licensing Terms

- **Commercial Software –** proprietary software that you commonly use. Has very restrictive rights on use.
- **Shareware/Trialware/Nagware** – a trial version of a commercial program. Can sometimes contain malware.
- **Freeware** – free in terms of price. No cost but can sometimes contain malware.

Software Licensing Terms

- **Open Source** – allows anyone the liberty to use, extend and distribute the software as they see fit. No Nag/Grey/Ad/Badware.
- **Free Software** - allows anyone the liberty to use, extend and distribute the software as they see fit. Focus on freedoms/liberty above all else. No Nag/Grey/Ad/Badware.
- **FOSS** – Free and open source software is a term to specify the range of free and open source software.

FOSS Programs

- Open Office - Office suite
- Ubuntu Linux - Entirely free operating systems.
- Mozilla Firefox - Open source browser.
- Wikipedia list of Open Source Applications
- Open Source Alternative
- OSSWIN - List of Open Source for Windows

Who creates this stuff?

- Where does it come from?
- Why do the create it?
- Myth vs. Reality

Hackers?

Hackers

- **Hackers** are not the media tells us they are.
- **White hat** = Good. Often called ethical hackers who help society, law enforcement and government.
- **Grey hat** = Middle of the road, sometimes good sometimes bad.
- **Black hat** = Compromised ethics and often criminally minded.
- **Hacker** in the technical and engineering community really means a person who wants to learn and understand something.

Crackers

Correct term is cracker, black hat or cyber criminal.

Cracking Demo/Psychographic

- Today it is less of teens just “messing around” like the movie War Games.
- Real threats are: criminal syndicates, foreign governments, general thugs.
- These organizations are the “well-source” of most of these activities.

Cracking Demo/Psychographic

- Motive (Money), Opportunity (Unpatched, insecure systems/network), Means (Resources).
- Crackers use increasingly sophisticated software to mount attacks.
- Malware consistently evolves around the attempts to defend against it.
- Evolves around technologies and delivery mechanisms. If SPAM filtering gets too effective they move to IM.

Cracking Demo/Psychographic

- Increasingly - malware have advanced characteristics: distributed, polymorphic, automatically evading detection, encrypted, self-protecting and self-healing.
- Shows all the hallmarks of professional software developments but with a deeply pernicious/evil intent.

The numbers speak...

Statistics.

Cyber Crime Stats

General Stats

FBI Computer Crime Survey 2005

Frequency of attacks. Nearly nine out of 10 organizations experienced computer security incidents in a year's time; 20% of them indicated they had experienced 20 or more attacks.

Types of attacks. Viruses (83.7%) and spyware (79.5%) headed the list. More than one in five organizations said they experienced port scans and network or data sabotage.

Financial impact. Over 64% of the respondents incurred a loss. Viruses and worms cost the most, accounting for $12 million of the $32 million in total losses.

Sources of the attacks. They came from 36 different countries. The U.S. (26.1%) and China (23.9%) were the source of over half of the intrusion attempts, though masking technologies make it difficult to get an accurate reading.

Reporting. Just 9% reported them to law enforcement.

Cyber Crime Stats..

Malware Stats

According to a study from TrendMicro -

It is estimated that PC Viruses cost businesses approximately $55 Billion in damages in 2003.

The same calculations in were done in 2002 and 2001, at $20-30 Billion and $13 Billion, respectively.

According to vendor Sophos -

In 2007, they uncovered 9,500 new infected web pages daily - an increase of more than 1000 every day when compared to April. In total, 304,000 web pages hosting malicious code were identified in May.

According to Anti-malware vendor Panda Labs -

Approximately 11 percent of computers around the world are part of these botnets, and they are responsible for 85 percent of all spam sent. In 2007, PandaLabs uncovered several tools such as Zunker or Barracuda, which were being used by cyber-criminals to administer networks of thousands of infected computers across more than 50 countries.

Cyber Crime Stats

Malware Stats

- **According to Gardner** - It is estimated that between May 2004 and May 2005, approximately 1.2 million computer users in the United States suffered losses caused by phishing, totaling approximately US$929 million. United States businesses lose an estimated US$2 billion per year as their clients become victims. In 2007 phishing attacks escalated. 3.6 million adults lost US $ 3.2 billion in the 12 months ending in August 2007.

Security is not

All about technology!

It's about what you do.

- Computer security is as much about what you do as it is about technology.
- Being aware of how to safely operate your computer is step one.
- The right technology with proper application of that technology is only part of the equation.

Social Engineering

- Cyber criminals will attempt to manipulate, finesse, trick the information from you in the most conniving and creative ways.
- Comes in the form of calls, emails, IM's, etc.
- Don't trust them. Don't give them information.
- ATT's Anti-social Engineering Training Vid

Web Fundamentals

Fundamental Technical Concepts/Terms

DNS

- Domain name system.
- It translates the underlying IP or numeric addresses of the internet into humanly readable form.
- I.e. www.google.com and not 74.125.47.147
- .com, edu, .gov, .mil. .au (Australia), .de (Germany), .it (Italy).

Domain name

- Domain name locates an organization online.
- GTLD (Generic Top Level Domains). Class of organizations. Ex. .com, .net, .gov.
- CcTLD (Country Code Top Level Domain). Country or territory. Ex. .us (USA), .it (Italy)

Anatomy of web address

- URL – Universal Resource Locator or URI Uniform Resource Identifier.
- Web address
- http://en.wikipedia.org
- Protocol – http, https, ftp, etc.
- Hostname – name of machine.
- Domain name - .org - non-profit

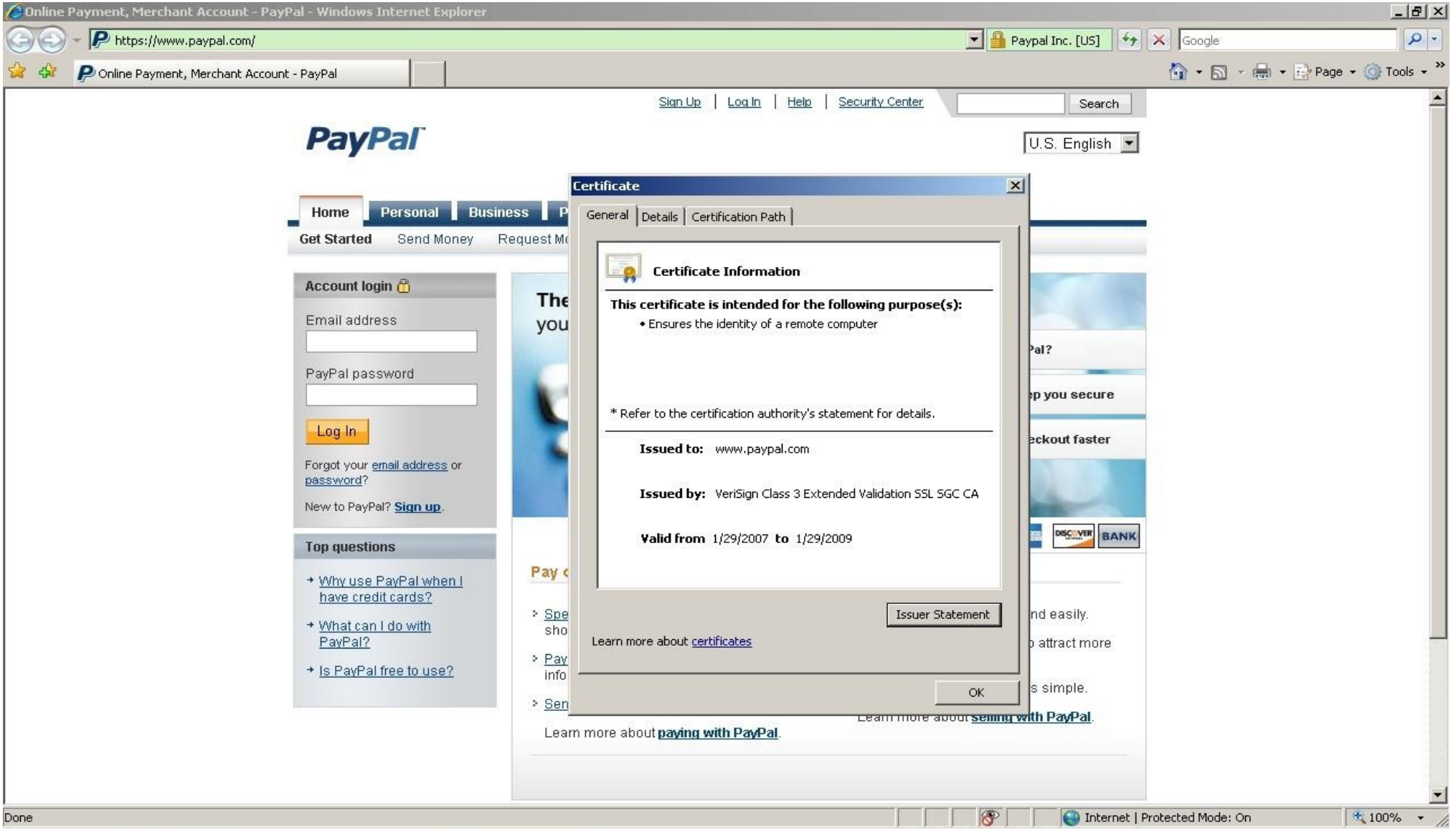
Anatomy of a web address
SSL

- Https
- SSL/TLS
- Secure encrypted web connection. Shows up as a lock in the browser.
- Don't enter in Personal Identifiable Information or engage in commerce without it!

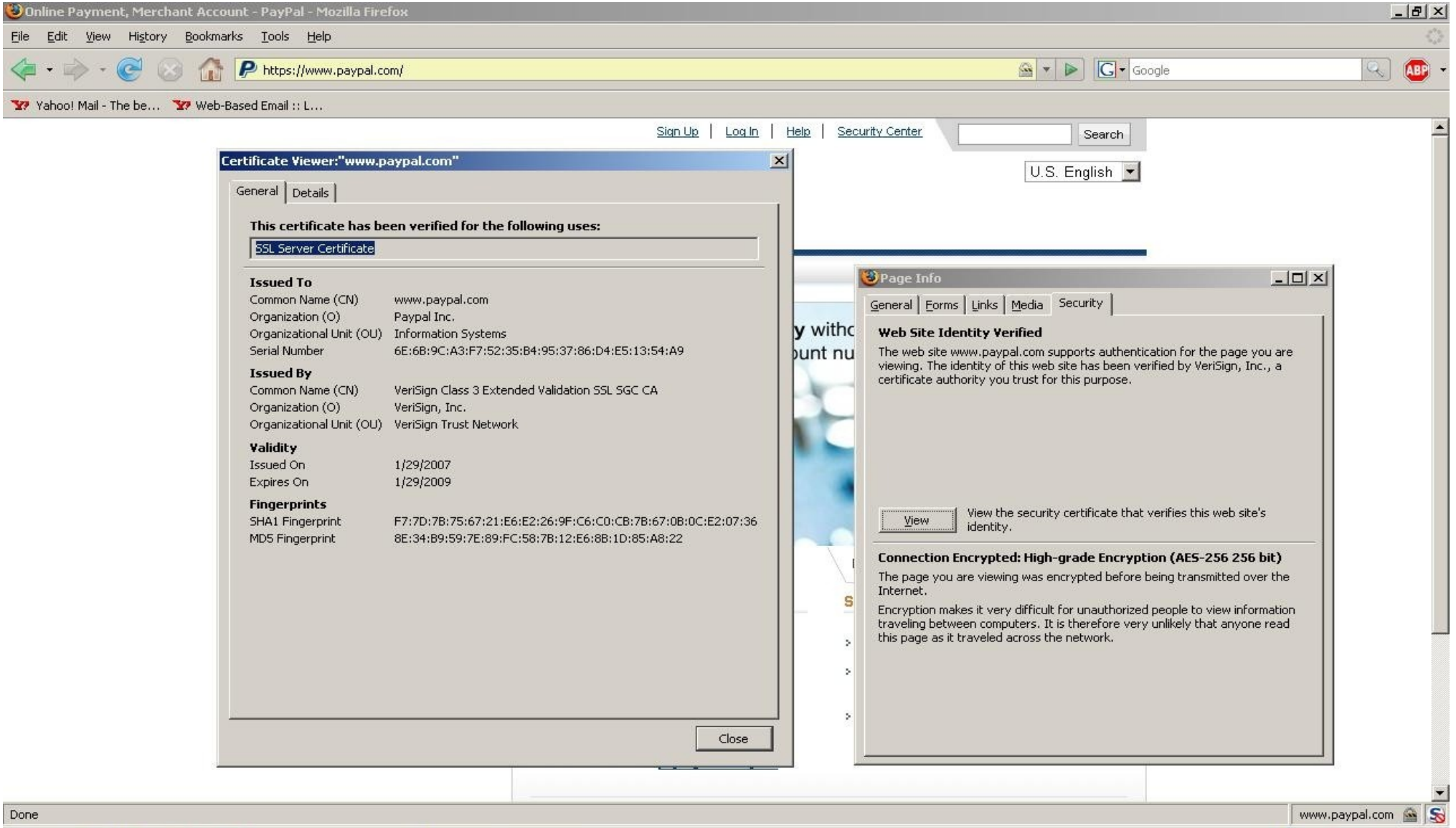
Anatomy of a Digital Certificate

- Much like a drivers license or other form of ID.
- Issued by Certification Authority such as Verisign, Thawte, GeoTrust, Entrust, Comodo or Godaddy.
- Validates that the website you are connected to.
- Look for the Lock!

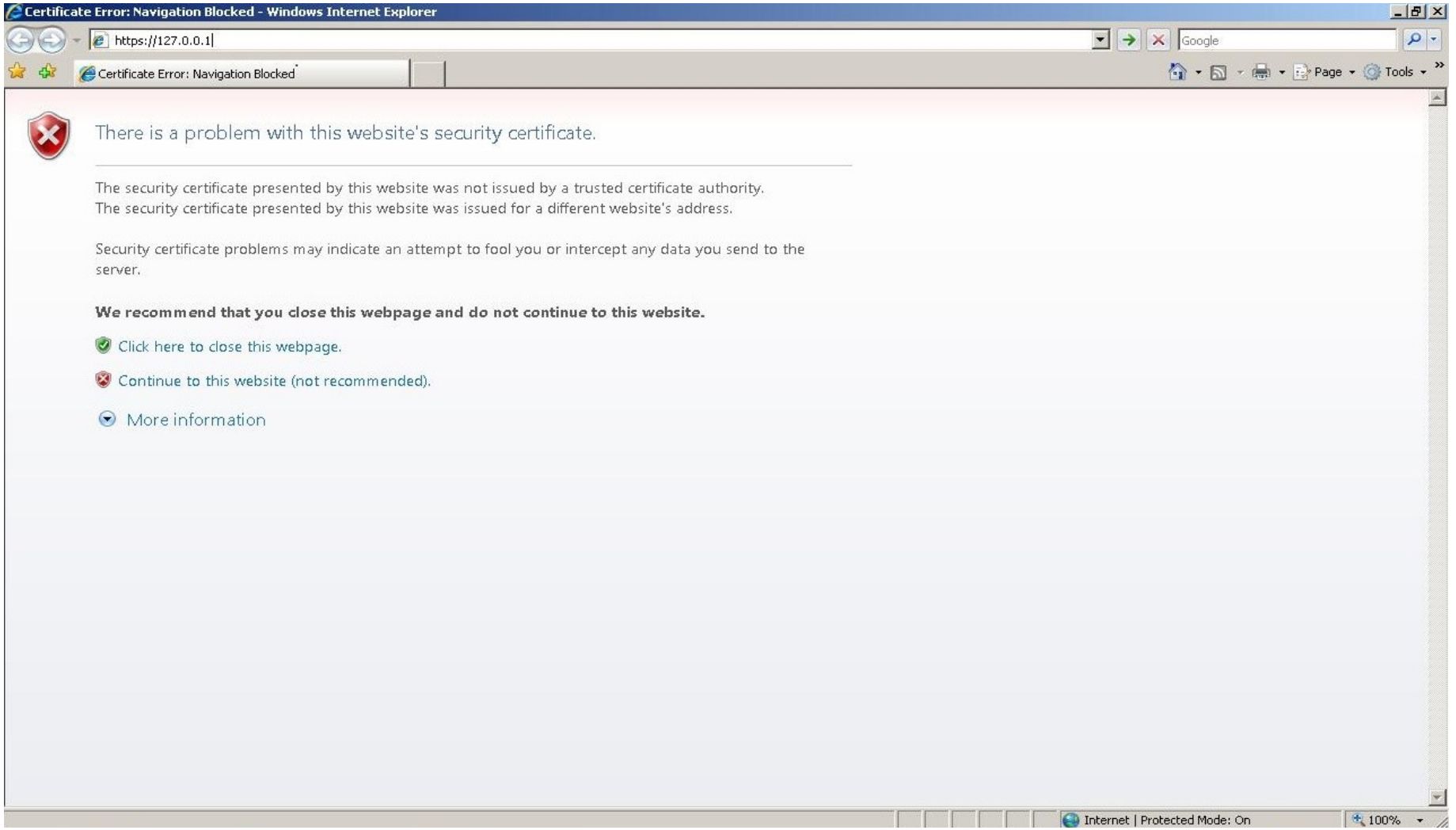
Internet Explorer 7 SSL Example
Valid Certificate



Firefox 2.x SSL Example
Valid Certificate

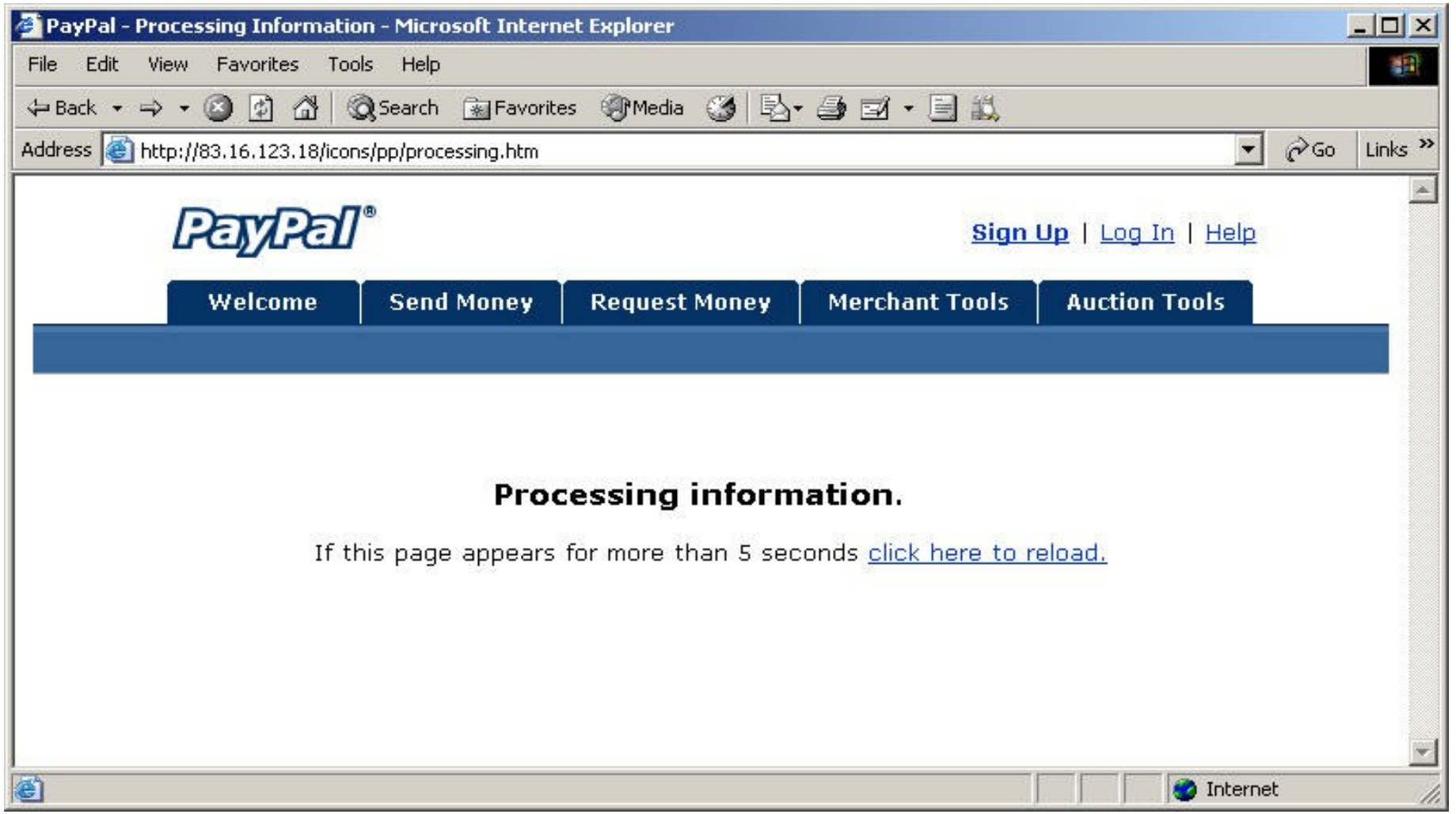


Internet Explorer 7 SSL Example Error!



Firefox 2.x Example
Error!

Internet Explorer SSL Example Fraudulent

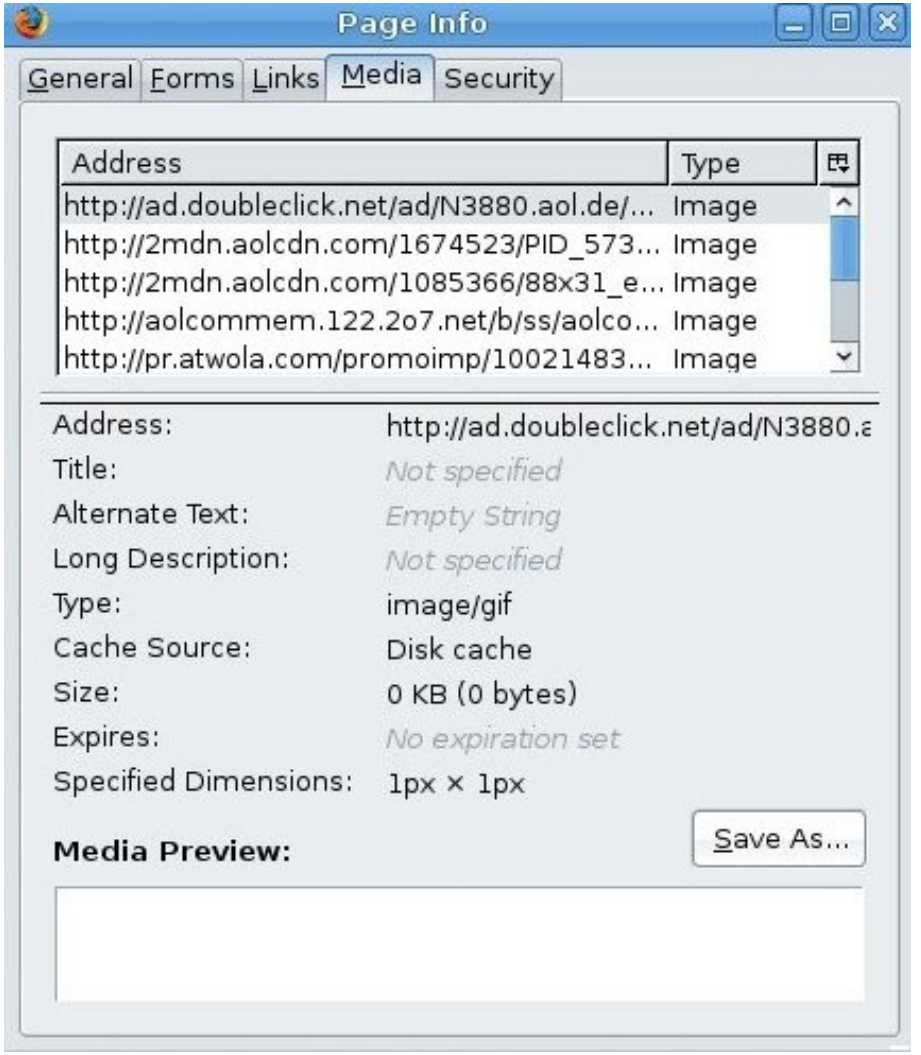


Anatomy of a web request

- When you visit a website your browser makes numerous requests for resources.
- Webservers are the internet resources that pass content of a website to your browser.
- These resources can be from many different websites some of which are not a part of the website in question.
- Some of this content driven by these third parties (ad networks, affiliates) may be infected or ads that lead you to be infected.

Anatomy of a web request

- Ex. http://www.aol.com
- In Mozilla Firefox go to Tools >> Page Info.
- doubleclick.net, aolcdn.com, 2o7.net, atwola.com, etc.



Web Threats

What are the threats?

Web Surfing Threats

- Malware is often delivered via websites clandestinely without your knowledge or approval.
- Phishing can redirect you to false websites that are used to harvest your login/password, credit card info, general identity information.
- If you don't know how to spell the name of an organization refer to company literature or Google, Yahoo, MSN.
- Browser based attacks are increasingly common. This type of attack pinpoints vulnerabilities in the browser software itself and it associated plug-ins(Flash) or technologies(Java/Javascript). Expect this trend to continue.

Phishing

- SPAM brings you messages that seem to be from legitimate parties that send you to phony/look-alike website.
- Your (Personally Identifiable Information) and credit card information is collected and sold in the underground.
- Usually an attempt is also made to infect your machine with malware.
- Best to not even open. Delete.

Phishing Cont.

- Think before you click! Don't open. Delete it!
  - Are you a customer? - If not Mark as SPAM and delete.
  - Did you have any recent interaction with the company involved? - Don't open it. Deleted!
- INSTEAD, go to the official website Validate its certificate.
- Then log on to your account.

Phishing
Professional Criminals

- Phishing attempts are increasingly looking more real and like real legitimate emails.
- The data these criminals possess about you is often legitimately from data breaches and or illegal/illegitimate sources. So increasingly they can accurately make these look real.
- Phishing attempt on Executives.
- IRS Phishing Scheme.

Phishing Email Characteristics

- Grammatical/Typographical Errors – You purchases Ebay Item and late payment. Account cancel!
- Social Engineering – Attempt to mislead, persuade,confuse, etc.
- Generic or Targeted Greetings – Hello Distinguished Sirs!?
- Urgent Request for PII – We need to validate your account or you will be terminated from the internet!
- Forged Email. - Email is often not valid and or not from the domain in question.
- Incorrect Link – Link is obviously wrong. https://www.payppal.net/~noway

Phishing General Advice

- Paypal Anti-Phishing Guide
- Ebay Anti-Phishing Guide
- Phish Tank Website
- Anti-Phishing Working Group Archive

Web Surfing Remediation

- Only visit sites you can judge to be legitimate. If you are engaged in Ecommerce make sure certificate is valid.
- Trust not click not.
- Mistyping a URL can lead you to a fake/phishing or even malware site.
- Only go directly to the associated website via typing it in the location or address bar.

Web Surfing Remediation

- Install an up to date anti-malware suite.
- Use the existing anti-phishing tools in Vista (IE7) or OSX (Safari).
- Alternatively use such as Netcraft Toolbar or PhishTank.
- Keep you system patched.
- Stay away from the “underbelly” of the internet.

Websurfing
Secure your browser

- Microsoft Internet Explorer
  - Set up trusted zones.
  - IE 7 has anti-phishing filter.
- Mozilla Firefox
  - Optimally use Mozilla Firefox with AdblockPlus and PhishTank.
  - NoScript to block all executable content unless explicitly allowed.
- CERT Recommendations on Securing Browsers.

IM/Chat Threat

- Instant Messaging spammers send bulk IM (SPIM) with executables (programs), links and images.
- Threats to the Instant messenger software itself are common.
- Black Hat/Crackers/Cyber Criminals often send malware files, links, programs in chat rooms.
- Trusting people whom you have not met or know.

IM/Chat Remediation

- Don't click/open/execute messages, links, executables (programs) from sources you don't know or can validate EVER!
- Lock down your Instant Messenger settings to allow you only to receive messages from existing friends and or show you offline to all others. Granularity exists so use it.
- Update your Instant Messenger client when updates occur.
- Trust only those you truly can.

SPAM

Not that deliciously dubious “meat.”

SPAM Threats

- Spam is often a carrier/propagator of malware.
- Social Engineering is a common thread in SPAM.
- Spam and Phishing are interrelated activities.
- Spam contains beacons which spammers use to validate your email address.

SPAM Characteristics

- Grammatical/Typographical Errors – You purchases Ebay Item and late payment. Validate NOW!
- Social Engineering – Attempt to mislead, persuade, confuse, etc.
- Generic or Targeted Greetings – Good day sir!? Hello Mr. Joseph Guarino.
- Urgent Request for PII – We need to validate your account or you will be terminated from the internet!
- Forged Email. - Why would an @aol email be sending you a Paypal or Ebay notice?
- Incorrect Link – Link is obviously wrong. https://www.payppal.edu/~noway

SPAM Remediation

- Don't give out your personal email. Use a throw away free one for non-essential communications.
- Don't post your email address online on websites, forums, chatrooms, etc.
- Don't open spam! Use your email software to mark it as spam and delete it.
- Never respond to SPAM.
- Never EVER buy from SPAMMERS.

SPAM Remediation

- Most standalone email clients such as Outlook, Thunderbird and OS X Mail offer built-in SPAM filtering.
- Optimally shut off or limit; Images, Javascript, Java, Flash etc in your email client or web browser if you use web based email. Shut off HTML mail and use plain text.
- If you are getting lots of SPAM in your Inbox, switch to another email provider that does a better job.

Spam Example Themes

- **Lotto Scams** – You have won 4mill Pounds!
- **Job Offers** – Work at home 1/hr a day and make millions!
- **Ponzi schemes** – Pyramid schemes.
- **Found money** – Found $10/million US!
- **Stock scams** – Buy this great penny stock!
- **Education scams** – Scholarships and diploma mills.
- **Romance scams** – Foreign dating sites, you have a secret admirer. Olga really does love you, even though you have never met!
- **Financial scams** – Phony IRS communications, phony bank query, free credit report, free financial seminars.

Social Networking Threats

- Sites such as Myspace, Facebook, YouTube, Orkut, Xing, Ryze, LinkedIN.
- Cyber criminals use social networking sites as a delivery mechanisms for malware. Spammers and Malware purveyors use these sites features (email, IM, chat room) to “promote” less than reputable software and websites.
- Anonymous access to your account.
- Third party add-on applications may have security concerns.
- Fake accounts and spam content abound on some of these sites.
- Comment spam is a major problem on some of these sites.

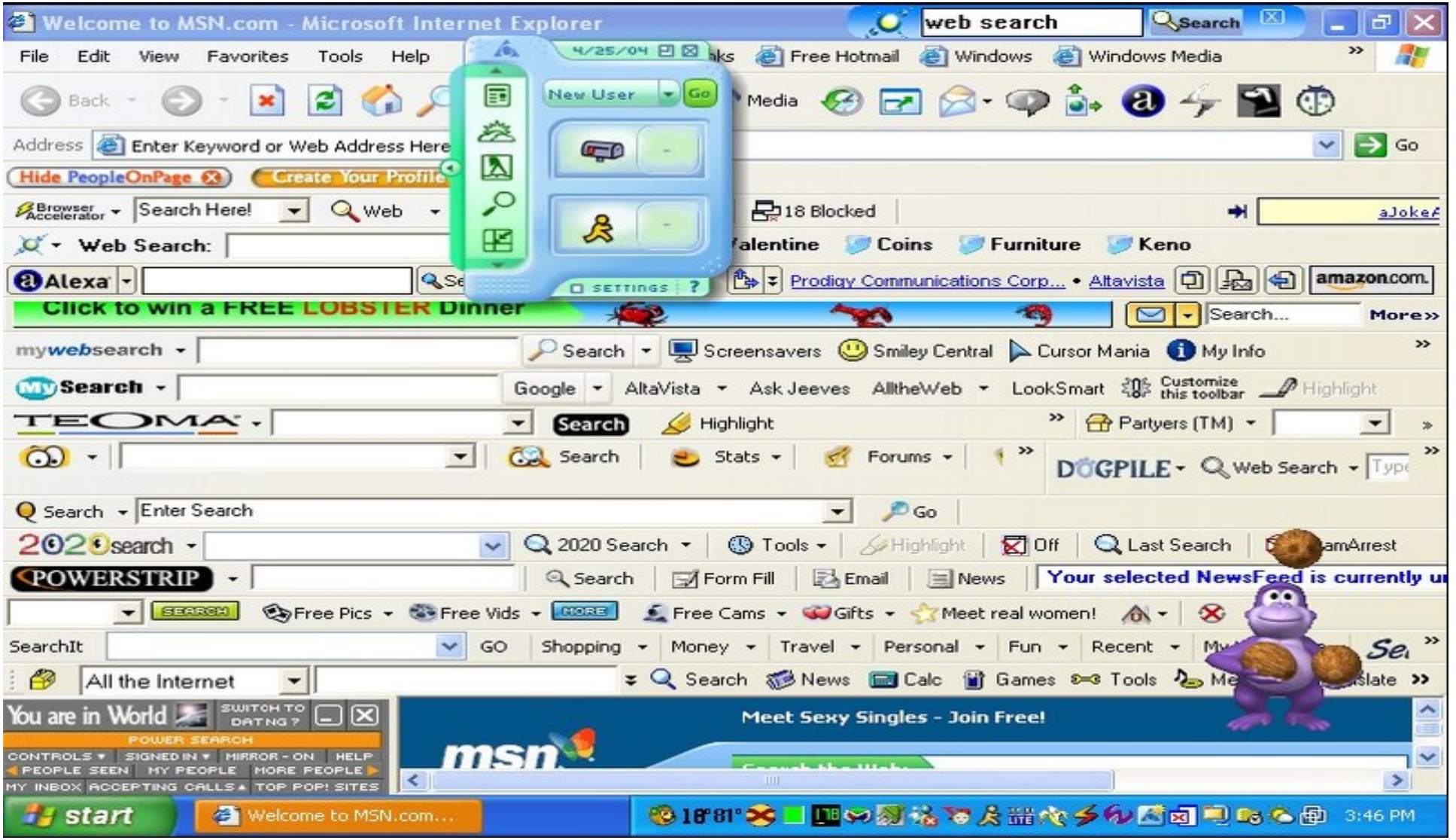
Social Networking Remediation

- If you don't know the person and have established a relationship with them then do NOT add them to your network.
- Delete or mark as SPAM, emails, IM's or comments that illegitimately advertise, or otherwise violate the sites terms of service.
- Don't click on content in people profile as it may redirect you to somewhere you don't want to go and or infect your computer with malware.
- Kids - Don't post anything you wouldn't want your parents, peers, or a potential employer to see. Remember cyber bullies and predators are a real threat.

Social Networking Remediation cont.

- Don't use third party add-ons. You can't validate these applications behavior, privacy policy, etc.
- Block anonymous access to your account.
- Shut off HTML and multimedia comments in your page.
- Report fake accounts so they can be removed. Community policing works!

Spyware/Adware/Badware/Greyware



Spy/Ad/Bad/Greyware

- Programs are shareware/freeware or arrive in spam, phishing, social network site, IM, etc.
- Trust not click not!
- Be in the habit of being skeptical!
- Research before you click or install.

Shareware/Freeware Threats

- Some shareware, Freeware are not technically free at all. Make sure to validate or research it first.
- They sometimes contain Adware, Spyware other programs that could damage your system, violate your privacy, cause data loss, or otherwise annoy you to tears.
- Ex. Wild Tanget, Bonzi Buddy, Weather Bug.
- Read the fine print.

Shareware/Freeware Remediation

- If you really need the program, buy from a respectable vendor.
- If you want a truly free program that has none of these problems - then get Free Software or Open Source Software.
- Read the fine print, EULA (End User License Agreement), Privacy Policy.

Blogging Threats/Remediation

- Spammers and malware purveyors have been automating spam postings to blogs for years.
- Only allow your approved comments.
- Don't post anything you wouldn't want your parents, peers, or a potential employer to see. Kids - Remember cyber bullies and predators are a threat.
- Block html, multimedia content from comments.
- Be careful what feeds you aggregate from other sites.

P2P Threats/Remediation

- P2P such as eDonkey, BitTorrent, Soulseek, etc.
- P2P networks are a great technology but the networks themselves often attract some shady elements of software piracy, malware purveyors, cyber-criminals.
- Don't download pirated copyrighted music, movies or programs unless you a want a free malware infection.
- Trust not click not.

Virtual Worlds Threats/Remediation

- Virtual Worlds such as Second Life, IMVU, There, Active Worlds and Kaneva.
- Social engineering can coax users into download or executing malware.
- Weaknesses in application can lead to malware infection.
- Update your Virtual World application when updates are available.

Gaming Threats/Remediation

- Gaming in an online context is as vulnerable as any online technology.
- Vulnerabilities and bugs in the games themselves are often exploited.
- Game servers can deliver malware to your machine.
- Other users can send links/IM's to malware.
- Update your game when patches or updates become available.

Web Forums Threats/Remediation

- You may be socially engineered to post personal information from forum members.
- Never post Personal Identifiable Information for any reason.
- If you post questions of a sensitive nature limit or sanitize this information.
- Forums can contain links to malware.
- Don't download files from web forums as you cannot trust or validate the source.

Other Threats

Other threats in cyberspace.

Cyber stalking

- Cyber stalking – misuse of information or communications technologies to harass another person, group or organization.
- Can involve threats, identity theft, monitoring, false accusations, damage to property or generalized harassment.
- Keep a digital log of all harassing communications.
- Lock the user out with your software settings. Block them.
- Report them to the website in question as a violation of the Terms of Service.
- Contact law enforcement if the problem persists.

Cyber stalking help

- WiredSafety.org
- National Center for Victims of Crime
- Working to Halt Online Abuse

Cyber bullying

- Targeted harassment or bullying using communication or information technology.
- Threats, pejorative labels, sexual remarks with intent to cause emotional/psychological distress.
- Lock the user out with your software settings. Block them.
- Report them to the website in question as a violation of the Terms of Service.
- Contact law enforcement if the problem persists.
- Kids - Talk to your parents, guidance councilor, whoever you really can trust.

Cyber bullying help

- Cyberbullying.org
- Cyberbullying.us
- Center for Safe and Rsponsible Internet Us

Online predators

- Don't trust anyone you meet online.
- Misrepresentation is common. A 50 year old man has the profile of a 16 year old.
- Don't ever give your personal information (name address, email, phone, social security number) to someone you meet online.
- Don't meet in person.
- Kids – Talk to your parents, guidance councilor, whoever you really can trust.

Online preditors

- Kids' Internet Safety Alliance
- NetSmartz
- FBI Guide to Internet Safety
- Microsoft guide to minimizing risk of online

Advice for

Parents.

General Advice for Parents

- Talk with your child about allowed internet uses. Establish known guidelines that set your expectations as a parent. Even written ones!
- Ask to review their online profiles. Remind them to think before posting or otherwise communicating anything that their parents, principal or nearly anyone of the billions of internet users can see it.
- Make your kids aware of what to do if they have a problem with cyber bullying, cyber stalking, preditors or otherwise.

General Advice for Parents cont.

- Keep the computer in a central location in your house. Not in their room.
- Block or limit other mobile/digital device access to the internet. I.e. Cell phone, PS2, etc.
- Install a hardware firewall that supports content filtering so you can block sites and content you don't want your children visiting.
- Consider installing monitoring software.
- Set them up with a limited account.
- Maintain an open, honest, respectful dialog

General Advice for Parents
Parental Control Software

- Web Watcher -
- http://www.webwatcherkids.com/
- Spectator Pro – PC/Mac -
- http://www.spectorsoft.com/index.html
- Net Nanny -
- http://www.netnanny.com/
- General List -
- http://en.wikipedia.org/wiki/List_of_Content_Control_Software

General Advice for Parents
Parental Control

- Both Windows Vista and OS X have built in Parental Control.
- All of these tools are relatively effective but not perfect.
- Optimally you should additionally block at the network level.
- Make sure your firewall/wireless access point supports parental controls as well.

General Computer Security Recommendations

General Internet Security Recommendations

Best Defense

Defense in depth – Using many layers, technologies, techniques and processes to help mitigate/reduce the risk of any one component of an information systems being compromised.

General Recommendations - Systems

- **Backup** your data to external disk, CD, DVD and or internet backup (encrypted in transit and at rest).
- **Patch** your system. Windows (Windows Update), Apple OSX (Systems Update). Set to auto update!
- **Patch third party applications**. Currently there is no common patch framework.
- **Least privilege**. Run as regular user not Administrator/ Root. Windows (Standard User), OSX (Standard User).
- **Use strong passwords**. >8 alphanumeric characters, not a word in any language.

General Recommendations - Systems

- **Buy an Anti-malware scanner.** Make sure it covers ALL malware threats! Buy a new one annually.
- **Don't run EOL (End of Life) software**. Ex. Windows 95/ME or Apple OS 8/9.
- **Trust not, click not**. Trust nothing unless you can validate its source.
- **Don't read/open/click** on spam, phishing emails, IM's, websites, content that you do not know or trust.
- **Encrypt** where required on any sensitive data.

The word on Anti-Malware Suites

- Buy only from vendors that offer a comprehensive suite of tools to combat todays threats.
- Anti-Malware suites are based on engine (brain) and DAT files (signatures).
- Behavior based are a step ahead because they look for anomalous (strange) behavior.
- An old anti-malware tool is a good as no anti-malware tool.

A word on passwords

- Choose strong passwords. >8 alphanumeric, not a word in any language. Use mnemonics or “memory device”.
- Strong passwords for you systems, websites, network devices, etc.
- There are also simple biometrics or a password management applications such as Robo Form or KeePass.
- http://www.us-cert.gov/cas/tips/ST04-002.html

General Recommendations - Networks

- Deploy both software/hardware firewall. Most anti-malware suites have a software firewall in them.
- Hardware firewalls from Linksys, D-Link, Netgear are inexpensive and generally effective.
- Many of these offer “content control” or “parental control” features to block objectionable content, etc.
- Update your firmware. See vendor site for details.

General Recommendations – Public Access Wifi – at home

- If you have wireless at home don't use WEP, use WPA or WPA-2.
- Change the password to access web interface.
- Set up WPA/WPA2 PSK (pre shared key) at the very least with a very long PSK (>33 characters).
- Update your firmware (software on the device). See vendor site for details.

General Recommendations
Public Access Wifi

- Check with the hotel, conference, coffee shop for the valid SSID or network name.
- Validate that you are connected to the right network. Check the certificate.
- Don't connect to random access points for “free internet” as you may become a victim of cyber criminals.
- Use a VPN (Virtual Private Network) if the information resource you are connecting to is of any importance.

Video on Cyber Security

- FBI on cybercrime
- BBC World on Europe's Cybercrime Convention
- Basics on Botnets
- Social Networking and ID Theft Risks
- Trendmicro Explains Malware
- Trendmicro on Computer Security 101

Another Angle

Industry

Industry/Legal/Regulatory Issues

- Industry has little desire or incentive to self-regulate.
- Consumers demand matters more to future improvements in technology.
- So only buy the products that meet your privacy/security needs.
- Regulation and legal frameworks need to catch up or be written with potential future technologies in mind.

Privacy

A simple practical guide to online privacy.

Common Misperceptions

Most believe that they have privacy in online activities....

Nope!

Orwellian present has been here for awhile...

Why is privacy important

- It's a human right.
- Fundamental to a democratic society.
- Assures our right to free speech, free assembly and a free press.
- Helps hold a balance of power between individual and industry/government.

Why privacy is important

- Our lack of privacy leads to abuses, crime, and real negative societal consequences.
- Real social, political and economic costs.
- United States citizens want more privacy from government and industry. http://epic.org/privacy/survey/

Stats

- In 2006, 14 million Americans were victims of identity theft.
- According to the Privacy Rights Clearinghouse, more than 330 data loss incidents involving more than 93 million individual records have occurred since February 2005.
- Data breaches have cost companies an average total of $4.7 million, or $182 per compromised record, in 2006, according the "2006 Cost of Data Breach Study" from Ponemon Institute. That's up from $138 per record last year.

Legal Foundation

Its important to note.

Legal Foundation

In the time of the framers of the constitution
NONE of the technology of today existed.

Legal Foundation Cont.

- Law is not a static entity.
- Privacy laws needs to evolve to protect us and our needs as tax paying law abiding citizens.
- As the scope of what is private shrinks we need change sooner rather than later.

Interesting Quote

"A future in which privacy would face constant assault was so alien to the framers of the Constitution that it never occurred to them to call out privacy as an explicit right. Privacy was inherent to the nobility of their being and their cause."

Bruce Schneier

Current Privacy Law Basis

- 1928 – Olmstead v. United States – wiretapping case.
- Supreme Court Justice Louis Brandeis wrote in his opinion.
- “The makers of the Constitution undertook to secure conditions favorable to the pursuit of happiness. They conferred, as against the government, the right to be let alone. “
- Right to be let alone is a commonly used definition of privacy.

Current Privacy Law Basis

- Written in 1789, the Fourth Amendment to the constitution states:
- The right of the people to be secure in their person, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated and no warrants shall issue , but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or thing to be seized.

Current Privacy Law Basis

- 9th Amendment – unenumerated rights not explicitly listed do in fact exist, such as the right to privacy.
- 14th Amendment - nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

Current Privacy Laws Links

- CDT - Privacy Laws
- PrivacyRights.org General Links
- EPIC.org - State Privacy Laws
- Wikipedia - Privacy Laws
- Wikipedia - Information Privacy Laws
- Wikipedia - Internet Privacy Laws

Back to cyberspace

Cyber privacy to be exact

Where should I worry about privacy?

- Web Surfing
- Instant Messenging
- Chat Room/IRC
- P2P Networking
- Social Networking
- Online Banking/Finance
- Freeware/Shareware
- Search Engine
- VoIP
- Gaming
- Blogging
- Wiki's
- Everywhere

Types of privacy threats

- Fraud
- Identity Theft
- Financial Loss
- Implication in Criminal Activity
- Cyber Stalking
- Cyber bullying
- Denial of health care
- Work place discrimination
- Denial of employment

Weakest Link

- Just like security. Privacy has a weakest link and its not always technology.
- Your choices and decisions matter.
- Read privacy statements, terms of use.
- Follow data breaches. If a firm you work with doesn't seem to take privacy or its own security serious go elsewhere.
- Act in ways the preserve your privacy.

Who and Why?

Many parties are involved in mining and analyzing your online activities.

Criminal

- Criminals misuse many of these same technologies and business practices to violate your privacy.
- These have the financial means, expertise and are motivated by the same profit motives (however illegitimate.)
- Criminal data breaches are a major problem.
- Ex. Data breach data ends up on a underground market that is then used to personalize “email market” or phishing campaigns.

Commercial

- Commercial – Search engines, websites, “free” email/IM, social networking sites.
- Mining this data is a multi-billion dollar industry that brings you online and off line advertisements
- Online marketing represents a revolution in marketing that allows untold understanding of your demographic & psychographic profile.
- Companies that don't properly invest in security technologies or their proper implementation are not protecting your privacy.

Commercial

- Not all companies are against privacy rights. There are many ethical companies that do ethical marketing.
- Vote with your dollar.

Government

- Government is deeply involved in monitoring, analysis and mining of our internet/electronic activities.
- Sometimes beyond what most legal scholars would consider fair, objective, or even constitutional.
- Most legal scholars, technologists, citizens think we need big changes.
- Studies consistently show most American's want more privacy, checks and balances and due process.

Government

- Government is doing the best job it can and many of them care very deeply about our privacy.
- All it takes is a few to abuse a system without checks and balances..
- NSA Traffic Interception at AT&T
- FISA vs. US Constitution
- USA Patriot Act - Concerns
- Domestic Surveillance Debate

What do they do

With that data?

Data Mining

- Data mining is correlating data from multiple sources to arrive at an understanding or result.
- In the marketing world it allow firms to have a deep understanding of your demographic and psychographic profile.
- As a result they sell to you better.
- Or annoy you more... =P

Your personal data isn't yours

- Nearly all commercial entities that have your personally identifiable information (PII) claim ownership of your personal information.
- They utilize it, sell it to partners, share it with other organizations. Your information is a valuable and lucrative commodity.
- Marketing, Direct Marketing, Online Marketing, Telemarketing

What

Should we try to protect?

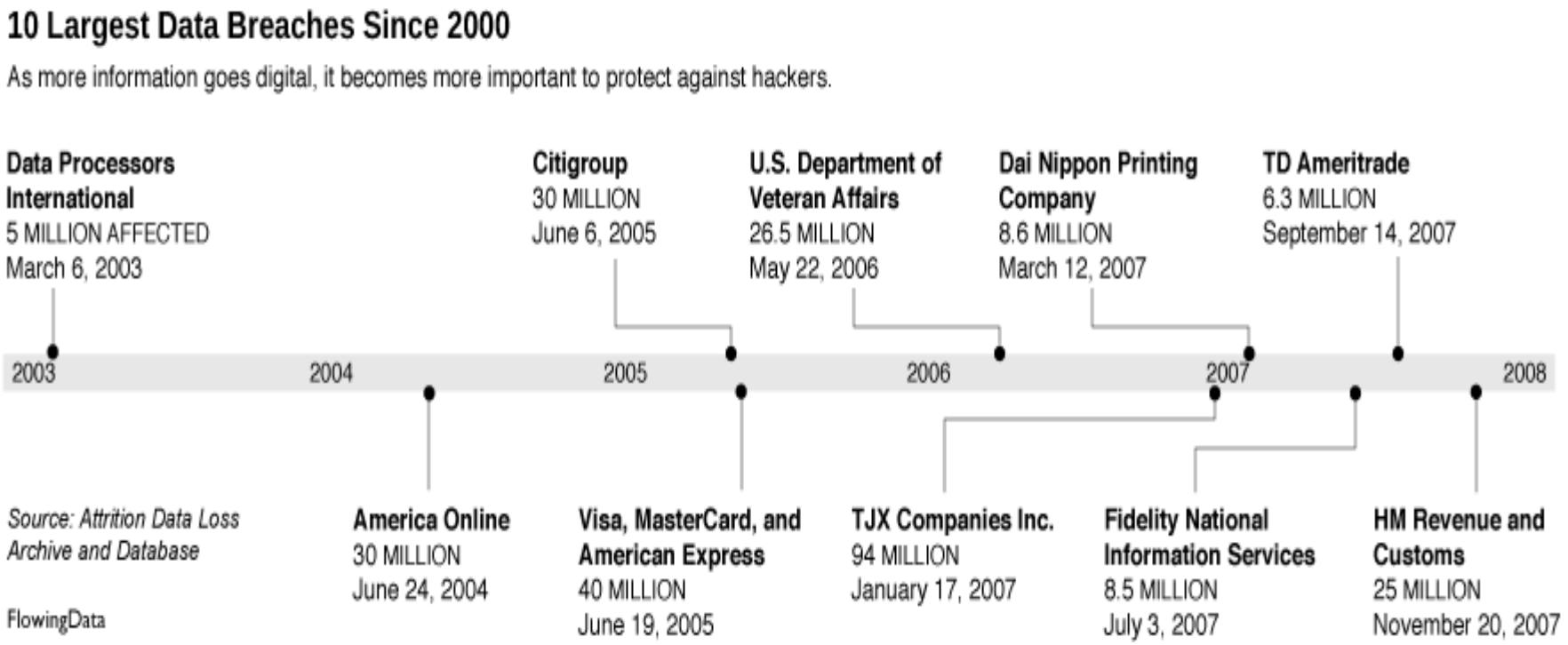
PII - Personally Identifiable Information

- Unique personal information used to identify you.
  - Full Name
  - Mother's maiden name
  - Banking information
  - Social security number
  - Credit card information
  - Address
  - Phone number
  - Password
  - Email addresses
  - Drivers License
  - Vehicle registration plate number

Data breaches and Privacy

- Data breaches or computer security breaches expand the threat to privacy.
- Data then ends up in the hands of the cyber-criminals who use it for nefarious ends.
- They sell this data in the criminal underground.
- Ex. Carding networks sell stolen credit card info.

Data Breaches since 2000



Also see: Privacyrights.org Chronology of Data Breaches

General

Cautionary Notes

General Cautionary Note
Adults

- Consider your interactions with the internet to be 100% public.
- Retention period is infinite.
- Recognize you no longer own it or control it.
- Minimize PII (Personally Identifiable Information)
- Don't post, IM, email anything you wouldn't want on a job application, employment record, or in the morning news.

General Privacy Recommendations Adults cont.

- Get in the habit of reading privacy statements and terms of use.
- Don't do business with companies that don't respect your rights.
- Don't be afraid to tell a company what you think needs to change. Ask to speak with the privacy officer or a manager/director of customer support. Give feedback and let you voice be heard.
- Support organizations that fight for privacy rights such as EPIC, EFF, CDT.

General Cautionary Note
Kids

- Think of your internet interactions as open for all to view.
- That will be kept online forever.
- Recognize you no longer own it or control it.
- Don't give PII (Personally Identifiable Information).
- Don't post, IM, email anything you wouldn't want on a job application, employment record, or in the morning news.

Web technologies

That effect privacy

Cookies

The not so delicious kind of cookie

- Tracking cookies are morsels of plain text sent back and forth between a server and your browser.
- Used in authenticating and tracking you as a website user and hold preferences and details and required for some functionality.
- First Party (Site you are visiting) vs. Third Party (Ad Networks)
- You can control the settings in browser settings.

Protecting your privacy
Web Surfing

- Remember you have little privacy while surfing the web.
- Your ISP has full transparent view of your activities.
- So do the websites, email services, search engines, instant messaging services, social networking sites.
- The sites that offer “free” services charge you with your PII (Personally Identifiable Information) and your privacy.

Protecting your privacy
Web Surfing

- Do not post, email, IM, or otherwise send/share PII (Personally Identifiable Information)
- Never email, instant message, post on a Wiki, Social Networking Site, in any form any of the following:
  - Banking information
  - Mother's maiden name
  - Social security number
  - Credit card information
  - Address
  - Phone number
  - Password
  - Email addresses

Protecting your privacy
Web Surfing

- If the information is not legally required i.e. its not a financial/government transaction then you don't need to provide it.
  Check state and federal law..
- Consider using an anonymizing proxy service such as Anonymizer.com,
  Hushmail Stealth Surfer, Tor or Jap.
- Optimally use Mozilla Firefox with AdblockPlus and NoScript to block all executable content unless explicitly allowed.

Protecting your privacy
IM/Chat

- No privacy of these communications.
- Privacy of your messages is not assured.
- 3rd parties can eavesdrop.
- Free service can further mine these for building a consumer profile on you.
- Many do support encryption (Yahoo, MSN).
- Encrypted Instant Messenger Clients - Wikipedia

Protecting your privacy
Social Networking

- Just as search engines, “free” email accounts and other websites mine your data so do Social Networking sites.
- More worrisome is that they create a climate in which people are willing to share details voluntarily they might not otherwise.
- They keep rich PII details.
- Be weary of the add on applications from social networking sites such as toolbars, IM clients.

Protecting your privacy
Social Networking

- Generally publicly available.
- Minimize PII.
- Don't use IM, Email or chat features if you are concerned with your privacy. No encryption and potentially infinite retention.
- Minimize posted to generally publically known information.

Protecting your privacy
Social Networking

- Post nothing sensitive or private EVER!
- Block your profile from public view.
- This doesn't really help your privacy from a marketing standpoint. It just keeps others from seeing your profile.
- Myspace Help Page

Protecting your privacy
Social Networking

- Join with a purpose. Friends/fun or business?
- Stick with that purpose and don't mix and match..
- If its for fun and friends then don't divulge more than you want to. You can use a pseudonym and comedic or otherwise obfuscated pictures.
- Don't post a picture that an Identity thief might be able to use. PII.

Privacy/Terms Policies

- Reading them might change your behavior.
- Facebook Terms of Use
- Facebook Privacy Policy
- Myspace Terms of Use
- Myspace Privacy Policy
- Youtube Terms of Use
- Youtube Privacy Policy

Example
Facebook

- Facebook Terms of Service
- By posting User Content to any part of the Site, you automatically grant, and you represent and warrant that you have the right to grant, to the Company an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to use, copy, publicly perform, publicly display, reformat, translate, excerpt (in whole or in part) and distribute such User Content for any purpose, commercial, advertising, or otherwise, on or in connection with the Site or the promotion thereof, to prepare derivative works of, or incorporate into other works, such User Content, and to grant and authorize sublicenses of the foregoing. You may remove your User Content from the Site at any time.

Example
Myspace

- Myspace Privacy Policy states that:
- MySpace also may share your PII with Affiliated Companies if it has a business reason to do so.
- Youtube Terms of Use states:
- For clarity, you retain all of your ownership rights in your User Submissions. However, by submitting User Submissions to YouTube, you hereby grant YouTube a worldwide, non-exclusive, royalty-free, sublicenseable and transferable license to use, reproduce, distribute, prepare derivative works of, display, and perform the User Submissions in connection with the YouTube Website and YouTube's (and its successors' and affiliates') business, including without limitation for promoting and redistributing part or all of the YouTube Website (and derivative works thereof) in any media formats and through any media channels.

Shareware/Freeware Privacy

- Can contain malware that might violate your privacy rights.
- If you really need the program, buy it.
- If you want a truly free program that has none of these problems - then get Free Software or Open Source Software.
- Read the fine print, EULA (End User License Agreement), Privacy Policy.
- If the vendor doesn't support the privacy you expect; go elsewhere.

Digital Restrictions/Rights Management Privacy

- DRM restricts the use of copyrighted material in ways not covered by existing law.
- DRM is a privacy risk when buying music, books, video and other content. Ex. Apple Itunes, Amazon Kindle.
- DVD's (CSS), Apple (Fair Play) Microsoft Vista (Protected Media Path), AACS for HD DVD/Blu-Ray.
- DRM and Privacy.

DRM
Continued

- Can be tracked to you as it sometimes contains meta data (name, account info, email).
- In the past you had some anonymity, freedom and even fair use.
- Not interoperable between devices and eventual obsolescence of your legitimately purchased content.
- Many in the legal community, technical, political see problems with it and the need for change. Steve Job's agrees with me. =P

What can I do to protect my privacy? online activities

- Read privacy policies and terms of use.
- Follow the computer security recommendations for your systems, network, etc. described above.
- Generally don't use commercial “free” email services without encryption.

What can I do to protect my privacy? online activities

- Use an anonymizing proxy services.
- Log out before using search engines/portals such as Yahoo, Google, MSN.
- Lock down your browser (detailed further in handout).
- Block or limit cookies..

What can I do to protect my privacy? online activities

- Don't fill in marketing surveys unless you agree with privacy policies.
- Encrypt sensitive data at rest on any and all digital devices.
- Don't buy closed technologies that contain DRM.
- Opt-out when you can.

Privacy

In the workplace

Privacy at work

- Don't assume your rights extend into the workplace.
- Don't expect privacy of any electronic communication.
- Companies have the liability, risks and responsibility for your behavior
- They want to shield themselves from financial and legal risk.

Privacy at work cont.

- Don't use company resource (communication resources) for personal use and expect privacy.
- Use your personal cell phone if its an emergency or you have something you want protected. You can do that off premises.
- Wait till you get home.

Encryption Choices

- Both Windows Vista and OS X support disk encryption.
- This provides encryption of the data at rest on your computer only.
- Microsoft Vista Bit Locker
- Apple File Vault

Encryption Choices

- PGP Desktop
- http://www.pgp.com/
- Veridis – Filecrypt
- http://www.veridis.com/
- Seganos Privacy Suite
- http://www.steganos.com/en/

Encryption Choices
Open source

- True Crypt
- http://www.truecrypt.org/
- GNU Privacy Guard
- http://www.gnupg.org/

Encryption
Email Providers

- Husmail
- http://www.hushmail.com
- xB Browser
- http://xerobank.com/xB_browser.html

Anonymized Surfing

- Anonymizer.com – provides anonymous websurfing, anti-spyware, secure erasure.
- Hushmail.com – Stealth surfer provides anonymous surfing.
- Tenebril GhostSurf– Anonymous surfing, anti-spyware, ad blocking, secure erasure.
- Tor Project – No cost anonymous internet surfing.

Secure Email
Personal Digital Cert

- Personal Digital Certificates – basically a digital ID.
- S/MIME – encryption for your email.
- Provides authentication, message integrity, non-repudiation, and privacy.
- Some providers offer free personal certificates.

Your digital trash

- When you recycle your old computer or (any other digital device) don't do it without securely erasing the data.
- Before you send it to recycling use Dban. http://dban.sourceforge.net/
- When you delete data its not gone. It can be easily recovered.
- Same goes for all other digital devices such as cell phones, personal assistants, etc. that have personal information on it.
- USB Thumb drive/Key, CD/DVD.

Secure Erasure Applications

- Microsoft Windows -
  - Eraser - http://www.heidi.ie/eraser/
  - Sysinternals - SDelete
  - East Tec – Eraser 2008
- Apple -
  - Apple – Secure Empty Trash/ Secure Erase
  - Smith Micro – Internet Cleanup
  - Apple OS X - SRM

The Paper Threats

- What goes out in the trash can lead to Identity Theft.
- Buy a shredder and use it.
- Opt out of junk email and credit card solicitations.

What can I do to protect my privacy?
Computer Security

- Keep your computer up to date/patched.
- Keep an updated anti-malware suite.
- Don't download freeware or shareware unless you have validated it is spyware, adware, greyware free.
- Buy the official release.
- Read the EULA (End User License Agreement) and Privacy Policy.

What can I do to protect my privacy?

- Read the privacy and terms of use policies of the firms you work with.
- Use a throw away email account with a pseudonym for non-critical communications.
- Give minimal information about yourself when its not required.
- Understand the legal rights firms have to demand certain PII information.
- Ex. If there is no state or federal law a firm shouldn't need your Social Security Number.
  US GAO Social Security - Federal & State Restrictions on use.

What we need moving forward

- Be involved.
- Choose to support companies that reflect your privacy/security needs.
- Vote with privacy, security in mind for digitally literate politicians. The internet is NOT a series of tubes!
- Comprehensive laws protecting privacy which is flexible enough to adapt to new technology.

What we need moving forward

- Laws like Europe Union.
- http://www.msnbc.msn.com/id/15221111/
- We should control our PII.
- We own our PII.
- We end up paying economic the social costs we shouldn't.

Opt out

- National Do-Not-Call List
- Mass Do Not Call List
- Opt-out Preapproved Credit Cards -
- FTC - Legitimate Free Annual Credit Report

Future Privacy Threats

- Genetic Testing
- RFID's
- Biometrics
- Real ID
- ISP monitoring and data mining
- GPS enabled cells

What we need moving forward
Industry Changes

- Self regulation doesn't work.
- Economic stats/studies prove this with consistency.
- Profit motive over all else. Just ask the C-level executives and shareholders!
- Regulation and legal frameworks must evolve!

Video on Privacy

- Jeffery Rosen - Is Privacy Dead
- Privacy and Social Networks
- Passport File Breach Presidential Candidates
- Got Privacy?
- Google Protecting Privacy on the Internet 07'

Conclusion

- Privacy and security are critical issues you can do something about.
- Its not all about technology. Its our choices and activities, laws/regulation, our political involvement **and** the technology .
- We can create a better world.

Big Thanks to:

- GBC/ACM
- Cambridge Science Fair
- Edward Freedman and David Presberg of the GBC/ACM
- All of you!

Creative Commons Licensed